UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,223	08/16/2001	Thomer Michael Gil	12221-007001	2855

26161 7590 10/20/2005

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
NAWAZ, ASAD M	

ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 10/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,223	GIL ET AL.	
	Examiner	Art Unit	
	Asad M. Nawaz	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21 and 50-77* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-21 and 50-77* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *7/25/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to the amendment received on 7/25/05. Claims 1, 12, and 21 have been amended. Claims 50-77 have been newly added. Claims 22-49 were previously withdrawn due to non-election. Accordingly, claims 1-21 and 50-77 are presented for examination.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 7/25/05 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

3. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-21 and 50-77 are rejected under 35 U.S.C. 103(a) as being unpatentable over Belissent (USPN 6789203) further in view of Vaidya (USPN 6,279,113).

As to claim 1, Belissent teaches a machine implemented method of monitoring traffic flow in a monitor device disposed to receive network traffic packets comprises:

producing statistics corresponding to a parameter of traffic flow to trace the source of an attack, (abstract; col 2, lines 55-65; the client's request rate is measured) with producing further comprising:

accumulating statistics from the packets (abstract; col 2, lines 55-65; the client's request rate is measured)

and comparing the number of buckets to a threshold (col 3, lines 6-36);

and determining whether the number of buckets should be divided into more buckets or combined into fewer buckets based on comparing the number of buckets to the threshold (col 2, line 49 to col 3, line 36; the rate of connections is compared to thresholds and appropriate action is taken).

However, Bellisent does not explicitly indicate mapping the traffic flow into a plurality of buckets by applying a hash function "f(h)" to the parameter of the traffic flow to output an integer corresponding to one of the buckets.

Valdya teaches mapping the traffic flow to a memory space by applying a hash function (col 3, lines 27-48; col 9, lines 3-20). It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate the teachings of Valdya into those of Belissent in order to make the system more organized. The organization

of the system using a hash function is known in the art. A specific hash function is used because its backward computation is difficult as well as its tendency to be collision free.

Claims 14, 21, 63, and 70 are essentially the method, computer program product, and the data collector for the machine implemented method of claim 1.

As to claim 2, Belissent teaches the method of claim 1 wherein the buckets are storage areas in a memory space of the monitor device. (col 3, lines 6-36)

As to claim 3, Bellisent teaches the method of claim 1 wherein as the number of buckets changes, the buckets have values derived from the buckets prior to the change. (col 2, line 49 to col 3, line 36)

As to claim 4, Valdya teaches the method of claim 1 wherein the hash function adapts to map to the new number of buckets, as the new number of buckets changes. (col 9, lines 3-45)

As to claim 5, Belissent teaches the method of claim 1 wherein comparing statistic values comprises: comparing the value accumulated in the bucket to a threshold that depends on the number of buckets. (col 2, line 49 to col 3, line 36)

As to claim 6, Bellissent teaches the method of claim 1 wherein the parameter is the count of how many packets a data collector or gateway examines (col 5, lines 4-20)

As to claim 7, Belissent teaches the method of claim 1 wherein as a value of a parameter for one bucket approaches a threshold, the monitoring device raises an alarm. (col 2, line 49 to col 3, line 36)

As to claim 8, Valdya teaches the method of claim 1 wherein the hash function changes periodically in a randomly secret manner so that packets are reassigned to different buckets (col 9, lines 3-45).

As to claim 9, Belissent teaches the method of claim 1 wherein the variable number of buckets dynamically adjusts the amount of traffic and number of flows monitored, so that the monitoring device is not vulnerable to a denial of service attack against its own resources (col 2, line 49 to col 3, line 36).

As to claim 10, Belissent teaches the method of claim 1 wherein the variable number of buckets efficiently identifies the source or sources of attack by breaking down traffic into different buckets and examining statistics accumulated for a parameter and a corresponding threshold in each bucket (col 4, lines 9-25).

As to claim 11, Belissent teaches the method of claim 1 wherein the traffic is monitored at multiple levels of granularity, from aggregate to individual flows (col 3, lines 6-36).

As to claim 12, Belissent teaches the method of claim 1 wherein the method is applied to monitoring of TCP packet ratios and repressor traffic. (col 5, lines 20-35)

As to claim 13, Belissent teaches the method of claim 1 wherein the threshold is a first threshold and the method further comprises: comparing accumulated statistic values from the buckets to second threshold values to determine that an event is of significance. (col 5, lines 45-52)

Claims 15-20, 50-62, 64-69, and 71-77 are essentially, the data collector, computer program product and the method for the machine implemented method of the above-mentioned claims.

Applicant's submission of an information disclosure statement under 37 CFR 1.97(c) with the fee set forth in 37 CFR 1.17(p) on 7/25/05 prompted the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 609.04(b). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Asad M. Nawaz whose telephone number is (571) 272-3988. The examiner can normally be reached on M-F 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on (571) 272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AMN

Bharat Barot

BHARAT BAROT
PRIMARY EXAMINER